DNV·GL

INDUSTRIELL IKT OG IIOT

Infrastruktur innen industrielle kontroll- og sikkerhetssystemer

Petroleumstilsynet

Rapport nr.: CyberSecurity/J-24/25154785/DNV, Rev. 1.1
Dokument nr.: 25154785/DNV
Dato: 2019-06-21

Prosjekt navn:	Industriell IKT og IIoT	DNV GL AS
Rapport tittel:	Infrastruktur innen industrielle kontroll- og sikkerhetssystemer	Control & Bridge Systems Postboks 300
Kunde:	Petroleumstilsynet, P.O. Box 599 4003 Stavanger Norway	1322 Høvik Norway
Kontaktperson:	Espen Seljemo	
Dato:	2019-06-21	
Prosjekt nr.:	10148973	
Organisation unit:	Security & Information Risk Management	
Rapport nr.:	CyberSecurity/J-24/25154785/DNV Rev. 1.1	
Dokument nr.:	25154785/DNV	

Kontrakt for leveranse av denne rapport:

Avtale om Systemer og Infrastruktur innen IKT og IIoT

Hensikt:

Utarbeidet av:	Verifisert av:	Godkjent av:
Pål Børre Kristoffersen Principal Specialist	Tore Hartvigsen Senior Principal Engineer	Jan Tore Grimsrud Head of Section, Control & Bridge Systems
Olav Haugehåtveit Senior Engineer		
Knut Omberg Principal Engineer		

DNV GL Distribution:

☒ Unrestricted distribution (internal and external)
☐ Unrestricted distribution within DNV GL
☐ Limited distribution within DNV GL after 3 years
☐ No distribution (confidential)
☐ Secret

Keywords:

Cybersecurity, Security, Digital Vulnerabilities, Oil & Gas, Information Risk Management, Lysneutvalget

Rev. Nr.	Dato	Formål	Utarbeidet av	Verifisert av	Godkjent av
0.6	2019-05-31	Høringsutkast	Pål Kristoffersen		
0	2019-06-14	Revidert etter høring	Pål Kristoffersen	Tore Hartvigsen	Jan Tore Grimsrud
1	2019-06-21	Oppdatering etter arbeidsmøte	Pål Kristoffersen	Tore Hartvigsen	Jan Tore Grimsrud
1.1	2019-07-05	Oppdatering etter kommentarer Ptil	Pål Kristoffersen	Tore Hartvigsen	Jan Tore Grimsrud

INNHOLD

1 SAMMENDRAG

Industrielle kontroll- og sikkerhetssystemer har vært en viktig forutsetning for olje- og gassproduksjon på norsk sokkel. Kontrollsystemene har muliggjort rask og effektiv kontroll og overvåkning av prosessene. Sikkerhetssystemene har sørget for å etablere sikker tilstand dersom feil eller andre uforutsette hendelser har inntruffet. Industrielle kontroll- og sikkerhetssystemer krever høy grad av sikkerhet både for å håndtere utilsiktede hendelser, men i økende grad også for å håndtere tilsiktede ondsinnede handlinger utført ved hjelp av datanett og datamaskiner.

Denne rapporten kartlegger infrastrukturen som er etablert for slike industrielle kontroll- og sikkerhetssystemer, og utreder fremtidige trender som tingenes internett og økende digitalisering av sektoren. Kartleggingen er basert på dokumentstudier og intervjuer med aktører i sektoren.

De industrielle kontroll- og sikkerhetssystemer som ble installert på de første installasjonene i Nordsjøen var primært leverandørspesifikke løsninger med både leverandørspesifikk maskinvare og programvare. Det ble primært benyttet dedikert kabling mellom sensorer, aktuatorer, kontrollere og det var ingen tilknytning til IKT-systemer. Problematikk knyttet til IKT-sikkerhet var ikke kjent eller tatt hensyn til.

For å redusere kostnader ble deler av de leverandørspesifikke løsningene skiftet ut med generelle IKT-komponenter. Feltbusser ble benyttet for å sammenkoble industrielle komponenter og tradisjonelle datanettverk ble benyttet for å sammenkoble kontrollere, brukergrensesnitt, vedlikeholdssystemer, kontrollrom, osv. Slike nettverksløsninger sparte kablingskostnader, de forenklet vedlikehold og muliggjorde bedre samspill mellom komponenter fra forskjellige leverandører. Kontrollrom ble forbedret med generelle dataskjermer og økende bruk av ekspertsystemer. Produksjonsdata ble i økende grad overført til IKT-systemer for produksjonsregnskap og analyse. Det ble etablert fiberoptiske nett på sokkelen og nye satellittbaserte tjenester for datatrafikk. Dette muliggjorde fjernvedlikehold av systemene. Flesteparten av installasjonene knyttet til norsk olje- og gassvirksomhet er basert på disse nyere industrielle kontroll- og sikkerhetssystemer.

Bruk av industrielle kontroll- og sikkerhetssystemer basert på «hyllevare» IKT-komponenter og økende bruk av kommunikasjon mellom forskjellige systemer medførte en økende bekymring for IKT-sikkerhetshendelser. STUXNET angrepet i ca. 2010 var en øyeåpner for at slike systemer er sårbare. Flere tilfeller av at løsepengevirus har spredd seg til industrielle systemer og det er oppdaget ondsinnet programvare som er laget for å skade sikkerhetssystemer. Nyere hendelser slik som LockerGoga angrepet på Norsk Hydro i 2019 viste at denne trenden fortsetter. Disse hendelsene medførte at en rekke aktører i norsk olje- og gassvirksomhet satte seg sammen og etablerte kravsett og beste praksis for å redusere risiko for IKT-sikkerhetshendelser.

Dagens beste praksis for industrielle kontroll- og sikkerhetssystemer består at tekniske tiltak, effektive prosesser og personell med god innsikt og kunnskap i temaet. De tekniske tiltakene baserer seg bl.a. på sonedeling av nettene og barrierer mellom sonene. Det er etablert veiledninger for å begrense og kontrollere all datatrafikk mellom IKT-systemer og operasjonelle systemer og videre for å begrense og kontrollere datatrafikk mellom industrielle kontrollsystemer og sikkerhetssystemer. De nye installasjonene som er bygget basert på denne beste praksis utgjør en liten andel av installasjonene.

Innføring av industrielle «tingenes internett» (IIoT) i olje og gass industrien har begynt med bruk av ikke kritiske sensorer for overvåkning og datainnsamling. Det forventes at denne utviklingen vil akselerere blant annet for å tilrettelegge for tilstandsbasert vedlikehold. Flere prosjekter er i gang med sensorer som overvåker roterende utstyr. Det er ikke identifisert prosjekter der kritiske kontrollsystemer eller sikkerhetssystemer vil ta i bruk slike mer intelligente enheter med internett basert kommunikasjon.

Det er ikke ønsket å innføre sikkerhetsmodeller basert på kryptering i kontroll- og sikkerhetssystemer. Utrullingen av IIoT enheter vil derfor skje i egne soner eller «siloer».

Mengden av produksjonsdata som overføres fra industrielle kontroll- og sikkerhetssystemer til tradisjonelle IKT-løsninger for analyse og simulering har over tid vært økende. Denne trenden vil akselerere og det vil tas i bruk mer avanserte analysemodeller basert på digitale tvillinger og kunstig intelligens. Infrastruktur for å transportere data ut av produksjonsanleggene er godt etablert, men det er forskjellige strategier for hvor data skal prosesseres. Det er et ønske om å benytte rimelige og høykapasitetsløsninger i skytjenester, men det er bekymringer for IKT-sikkerhet. Slike bekymringer er spesielt relevante når analyseplattformene skal optimalisere prosessanleggene og prosessinnstillinger skal endres i sann tid. Dette vil også utfordre de eksisterende løsningene for datatransport som er designet for å transportere data kun ut fra de industrielle kontroll- og sikkerhetssystemene.

2 ENGLISH SUMMARY

Industrial control and safety systems have been an important prerequisite for Norwegian oil and gas production. The control systems have enabled rapid and efficient control and monitoring of the processes and the safety systems have ensured the establishment of a safe condition if errors or other unforeseen events have occurred. Such industrial control and safety systems require a high degree of security both for dealing with accidental incidents but increasingly also for dealing with targeted malicious actions using computers and networks.

This report examines the infrastructure established for such industrial control and safety systems and examines future trends such as the Industrial Internet of Things and increasing digitalization of the sector. The discussions are based on document studies and interviews with actors in the sector.

The industrial control and safety systems installed on the first installations in the North Sea were primarily supplier-specific solutions with both supplier-specific hardware and software. Dedicated wiring between sensors, actuators and controllers was primarily used, and the control-rooms were built using custom panels. There was no connection to IT-systems and only radio communication was used for external communication. Issues related to cyber security were not known or taken into account.

To save costs, many supplier-specific solutions were replaced with general IT-components. Fieldbuses were used to interconnect industrial components and traditional computer networks were used to interconnect controllers, user interfaces, maintenance systems, control-rooms, etc. Such networking solutions saved cabling costs, simplified maintenance and enabled better interoperability of components from different vendors. Control-rooms were improved with general computer monitors and increasing use of expert systems. Production data was transferred to IT-systems for accounting and analysis. Fibre-optic networks and satellite-based services for data traffic were established. This has enabled remote maintenance of the systems.

The use of industrial control and safety systems based on commercial off-the-shelf IT-components and increasing use of communication between different systems led to an increasing concern for cyber security incidents. The STUXNET attack in 2010 was an eye-opener for such systems being vulnerable. Several cases of ransomware have spread to industrial systems and malicious software targeting safety systems has been discovered. A more recent incident such as the LockerGoga attack on Hydro in 2019 showed that this trend is continuing. These incidents have led to a number of actors establishing a set of requirements and best practices to reduce the cyber security risks.

Today's best practices for industrial control and safety systems consist of technical measures, efficient processes and personnel with good insight and knowledge in the subject. The technical measures are, among other things, based on implementing a zone-model and to establish barriers between the zones. Guidance has been established to limit and control all data traffic between IT-systems and operational systems and further to limit and control data traffic between industrial control systems and safety systems.

The introduction of "Industrial Internet of Things" into the oil and gas industry has begun using non-critical sensors for monitoring and data collection. It is expected that this development will accelerate, to facilitate condition-based maintenance. Projects are running to monitor rotating equipment. No projects have been identified where critical control systems or safety systems will deploy such more intelligent internet-based communication devices. It is not wanted to introduce security models based on encryption in control and safety systems. The roll-out of IIoT units will therefore take place in separate zones or "silos".

The amount of production data transferred from industrial control and safety systems to traditional IT-solutions for analysis and simulation has been increasing over time. This trend will continue, and more advanced analysis models based on digital twins and artificial intelligence will be used. Infrastructure for transporting data out of the production facilities is well established, but there are different strategies for where to process data. There is a desire to use affordable and high-capacity solutions in cloud services, but there are concerns about cyber security. Such concerns are particularly relevant when the analysis platforms are to optimize the processes and when process settings shall be changed in real time. This will also challenge the existing data transport solutions designed to transport data only in one direction from the industrial control and safety systems.

3 INNLEDNING

3.1 Bakgrunn

Digitalisering i olje- og gass-sektoren åpner opp for effektivisering, men gjør også sektoren mer sårbar for IKT-sikkerhetshendelser. Olje- og gass-sektoren er et mål for trusselaktører både på grunn av de store verdier sektoren representerer, men også for aktivister med idealistisk eller politisk motivasjon.

Selv om mange systemer og komponenter inngår i porteføljen til et olje- og gasselskap er det spesielt de industrielle kontroll- og sikkerhetssystemene som er viktig å beskytte. Ondsinnet kode eller ondsinnede endringer på systeminnstillinger kan i verste fall resultere i ødeleggelse av eiendeler, miljøkatastrofer og tap av liv. Det kreves god tverrfaglig kunnskap, styring og adekvate tiltak for å utnytte de mulighetene som den nye teknologien tilbyr, samtidig som den tilhørende risikoen blir vurdert og tatt høyde for.

Petroleumstilsynet gjennomfører en satsing på IKT-sikkerhet i perioden 2018-2021. Målet er å gå i dybden på en del viktige områder, innhente kunnskap om den teknologiske utviklingen og vurdere hvordan dette påvirker risikobildet. Tidligere er det publisert en rapport «Kunnskap IKT-sikkerhet og CERT» /1/ og det pågår en utredning om fjernarbeid og HMS.

Det ble lyst ut en konkurranse for å utrede Industriell IKT og IIoT, og dette oppdraget ble tildelt DNV GL.

3.2 Hensikt

Hovedmål for utredningen er å innhente kunnskap om infrastrukturer innen industrielle kontroll- og sikkerhetssystemer som benyttes til styring og overvåkning av ulike prosesser og systemer på innretninger, landanlegg og flyttbare rigger.

Oppgaven er å se på kompleksitet til disse systemene, levetid, oppbygning av infrastruktur og grensesnitt mot ulike typer nettverk inklusive kommunikasjonsprotokoller fra instrument/sensornivå til styre og kontrollnivå (HMI). IKT-sikkerhet og egensikkerhet til komponenter i den vertikale og horisontale akse er elementer som skal utredes.

Det skal også diskuteres hvilken utvikling og mulig påvirkning Industrial Internet of Things (IIoT) og andre trender kan ha på slike systemer når disse kobles til nettverksstrukturen.

3.3 Metodikk

For å utrede industriell IKT og IIoT, er det gjennomført litteraturstudier og innhentet erfaringer. Det er gjennomført intervju med aktører i sektoren. Dette inkluderer:

- Operatørselskap innretninger
- Teknisk tjenesteleverandør (TSP) landanlegg
- Boreselskap
- Leverandører av industrielle kontroll- og sikkerhetssystemer
- Leverandører av utstyr til olje- og gass-sektoren

Drøftinger, analyser og rapportskriving er basert på det innhentede materiale. Fakta for å belyse drøftingene og analysene er tatt med i egne faktabokser i rapporten.

For å fremheve hovedpoeng i rapporten er disse gjentatt og skrevet i uthevet skrift.

3.4 Forkortelser og definisjoner

BOP	«Blow Out Preventer»
CAP	«Critical Action Panel»
CERT	«Computer Emergency Response Team»
COTS	«Commercial off-the-shelf»
DMZ	«Demilitarized Zone»
DSB	Direktoratet for samfunnssikkerhet og beredskap
ESD	«Emergency Shutdown»
EWS	«Engineering Work Station»
F&G	«Fire and Gas»
GPS	«Global Positioning System»
GSM	«Global System for Mobile communication»
HMI	«Human Machine Interface»
IIoT	«Industrial Internet of Things»
IKT	Informasjon- og kommunikasjonsteknologi
IKT-sikkerhet	Sikring av IKT systemer. «Cyber Security»
IMS	«Information Management System»
IOGP	"International Oil and Gas Producers Association"
IT	Informasjonsteknologi
JD	Justis- og beredskapsdepartementet
MPLS-TP	«Multiprotocol Label Switching – Transport Profile»
NOROG	Norsk olje og gass
NOU	Norsk Offentlig Utredning
NSM	Nasjonal Sikkerhetsmyndighet
NVE	Norges vassdrags- og energidirektorat
OD	Oljedirektoratet
OPC	«OLE for Process Control»
OT	Operasjonsteknologi
OT-sikkerhet	Sikring av OT. Industriell IKT-sikkerhet.
PCN	«Process Control Network»
PLC	«Programmable Logic Controller»
PLS	Programmerbar Logisk Styring
PTIL	Petroleumstilsynet
RISI	«Repository of Security Incidents»
RTU	«Remote Terminal Unit»
SAS	«Safety and Automation System»
SIS	«Safety Instrumented System»
TCP/IP	«Transmission Control Protocol/Internet Protocol»
TSP	«Technical Service Provider»
UDP	«User Datagram Protocol»
USB	«Universal Serial Bus»
VPN	«Virtual Private Network»

4 INFRASTRUKTUR INNEN INDUSTRIELLE KONTROLL- OG SIKKERHETSSYSTEMER

Infrastrukturen innen industrielle kontroll- og sikkerhetssystemer har vært i sterk endring etter de første installasjoner på norsk sokkel. I dette kapittel beskrives kort utviklingen som har skjedd frem til i dag. Det er gjort en forenkling ved å skille mellom eldre systemer, nyere systemer og dagens beste praksis.

4.1 Eldre systemer

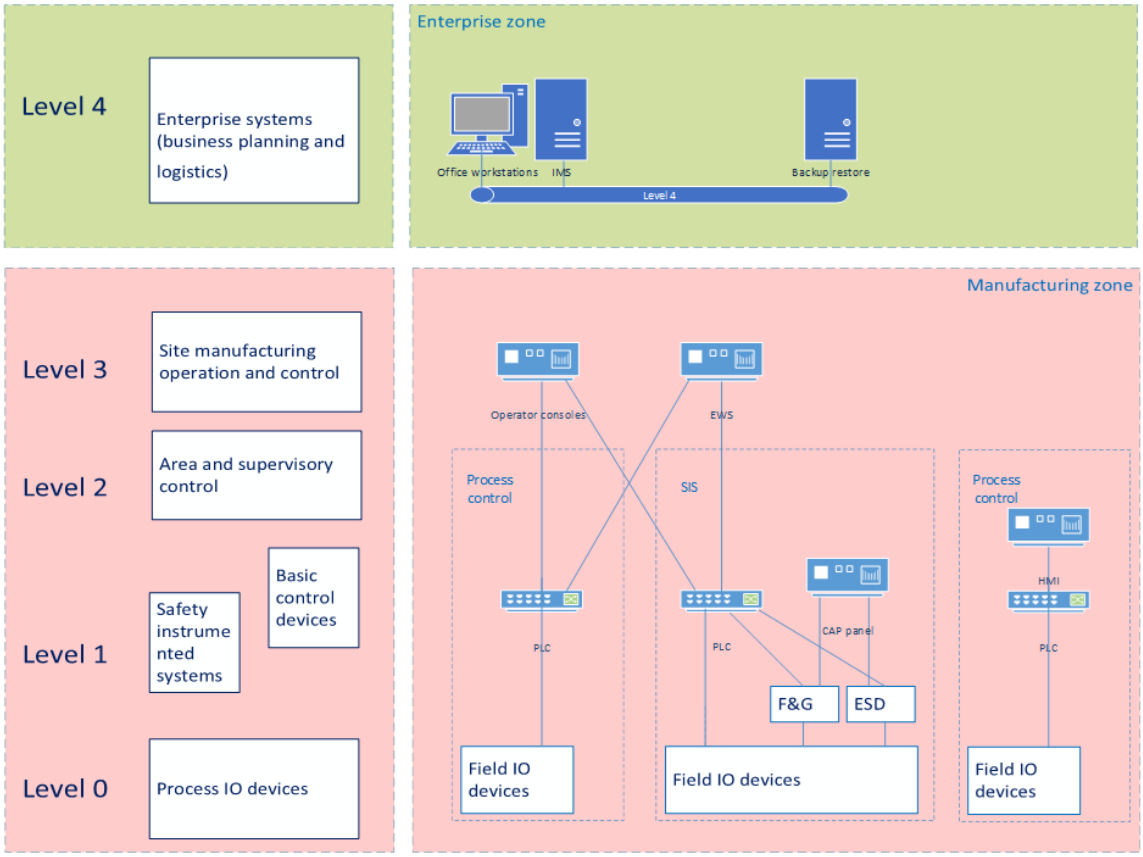
De første installasjonene på norsk sokkel som benyttet industrielle kontroll- og sikkerhetssystemer var i stor grad basert på leverandørspesifikk maskinvare og programvare. Selv om mange av disse installasjonene fremdeles er aktive, er de alle fleste industrielle kontroll- og sikkerhetssystemene oppgradert til infrastruktur som beskrevet i kapittel 4.2. Det finnes fremdeles større installasjoner og tredjepartssystemer som benytter industrielle kontroll- og sikkerhetssystemer basert på 20-30 år gammel teknologi.

«Det finnes fremdeles større installasjoner og tredjepartssystemer som benytter industrielle kontroll- og sikkerhetssystemer basert på 20-30 år gammel teknologi.»

Automasjonspersonell håndterte i hovedsak all infrastruktur, systemer, rutiner etc. selv, og der var liten samordning med de tradisjonelle IKT-disipliner. Siden de industrielle systemene var fysisk adskilt fra IKT-systemer («Air-gap») og operasjon og endringer av automasjonssystemene krevde fysisk tilstedeværelse på installasjonene var ikke IKT-sikkerhet et aktuelt tema.

4.1.1 Infrastruktur

Figur 1 viser skjematisk prinsippene for infrastruktur for de eldre systemene. Figuren er basert på Purdue modellen som er beskrevet i Faktaboks 1. I figuren er det illustrert et eksempel på industrielle kontroll- og sikkerhetssystemer fra en hoved SAS leverandør samt et isolert tredjepartssystem. Systemene var i stor grad basert på leverandørspesifikk maskinvare og operativsystem der eksempelvis Siemens leverte TELEPERM M familien og ABB leverte AC400 kontrollere.



Figur 1 – Infrastruktur og grensesnitt for eldre systemer

4.1.2 Nettverk og kommunikasjon

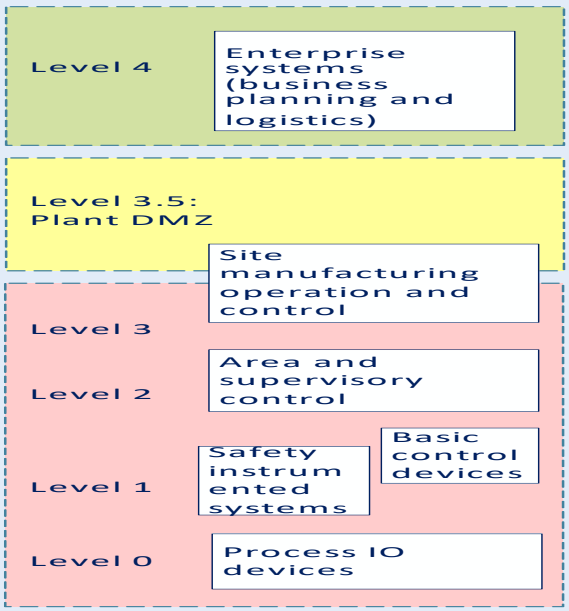
Sensorer og aktuatorer var typisk tilkoblet styresystemer med punkt til punkt dedikert kabling hvor signalene ble overført med konvensjonelle elektriske signaler (f.eks. ON/OFF, 4-20mA).

Proprietære protokoller ble ofte benyttet for kommunikasjon mellom PLSer, arbeidsstasjoner og annet utstyr fra samme leverandør.

Modbus RTU med grensesnitt RS-232, RS-422 eller RS-485 ble i noen grad benyttet for kommunikasjon med tredjepartsutstyr.

For kommunikasjon mot land og andre installasjoner, benyttet de første boreinstallasjonene på norsk sokkel radiosamband. For å oppnå høyere hastigheter over avstander lenger enn den optiske horisont, ble det etablert «tropochatter-samband» til Ekofisk installasjonene. I 1976 ble første satellittsamband (Norsat) etablert mellom landstasjon på Eik i Rogaland og Nordsjøen. Gullfaks feltet fra midten av 80 tallet fikk radiolinjesamband til land. Kommunikasjonssystemet ble først og fremst brukt til administrative formål, men fra slutten av 90 tallet fikk industrielle kontrollsystemer forgreninger til land /20/.

Purdue-Modellen



Purdue modellen /2/ ble utviklet av Theodore J. Williams og et konsortium ved Purdue universitet. Modellen brukes som referansemodell for å gruppere systemer og lage sonemodeller for å skille den fysiske prosessen fra forretningslogikk:

Level 0 Den fysiske prosessen
Level 1 Intelligente enheter
Level 2 Kontrollsystemer
Level 3 Produksjonssystemer
Level 4 Forretningssystemer

Senere er det introdusert et nivå 3.5 som en demilitarisert sone for å skille forretningssystemer fra produksjonssystemer.

Purdue modellen er ofte referert til når sikkerhetsutfordringer i sammensatte og komplekse IKT-infrastrukturer blir analysert.

Faktaboks 1 Purdue Modellen utvidet med level 3.5

4.1.3 IKT-sikkerhet

Så lenge de industrielle kontroll- og sikkerhetssystemene ikke var tilknyttet eksterne datanett, hadde de liten angrepsflate for IKT-sikkerhetshendelser. Leverandørspesifikke systemer basert på proprietær maskinvare og operativsystem var mindre kjent hos trusselaktører enn systemer f.eks. basert på Microsoft Windows, og utgjorde dermed en mindre risiko.

Det var ikke publisert standarder eller veiledninger i sikring av industrielle systemer mot IKT-sikkerhetshendelser.

Dette bildet endret seg når det ble utbygd nettverksløsninger på sokkelen og slike installasjoner ble integrert med andre systemer. Det ble gjerne etablert en ekstern brannvegg for å beskytte de industrielle komponentene, men kun en slik sone-barriere eller «skallsikring» er ikke ansett å være tilstrekkelig (se kapittel 4.3).

Oppdagelsen av ondsinnet programvare som TRITON (Se Faktaboks 7) har vist at trusselaktører også kan angripe proprietære systemer som benytter proprietære protokoller.

Det er også sikkerhetsutfordringer knyttet til at system kan være basert på programvare som ikke lenger har støtte («support») fra leverandørene. Eksempelvis er og det mange Windows XP baserte system i drift på sokkelen selv om det ikke lenger produseres sikkerhetsoppdateringer til denne plattformen.

«Eksempelvis er og det et mange Windows XP baserte system i drift på sokkelen selv om det ikke lenger produseres sikkerhetsoppdateringer til denne plattformen.»

Det er mange installasjoner der sensorer og aktuatorer for både kontroll og sikkerhet er knyttet til den samme kontroller og styres fra det samme brukergrensesnitt («HMI»). Det er god separasjon for essensielle sikkerhetssystemer som utblåsingssikring («BOP») og Brann & Gass.

«Det er mange installasjoner der sensorer og aktuatorer for både kontroll og sikkerhet er knyttet til den samme kontroller og styres fra det samme brukergrensesnitt («HMI»).»

4.2 Nyere systemer

Generelt kan man si at «nyere systemer» ble installert i perioden 2000 til 2016 og at de fleste systemene gjennomgikk et generasjonsskifte. For å spare kostnader begynte SAS leverandørene å bygge sine produkter basert på hyllevare («COTS»). Generiske PCer tilpasset produksjonsmiljø og generiske operativsystemer som Windows og Unix varianter ble introdusert i bl.a. kontrollrom, i brukergrensesnitt («HMI»), arbeidsstasjoner («EWS») og vedlikeholdssystemer.

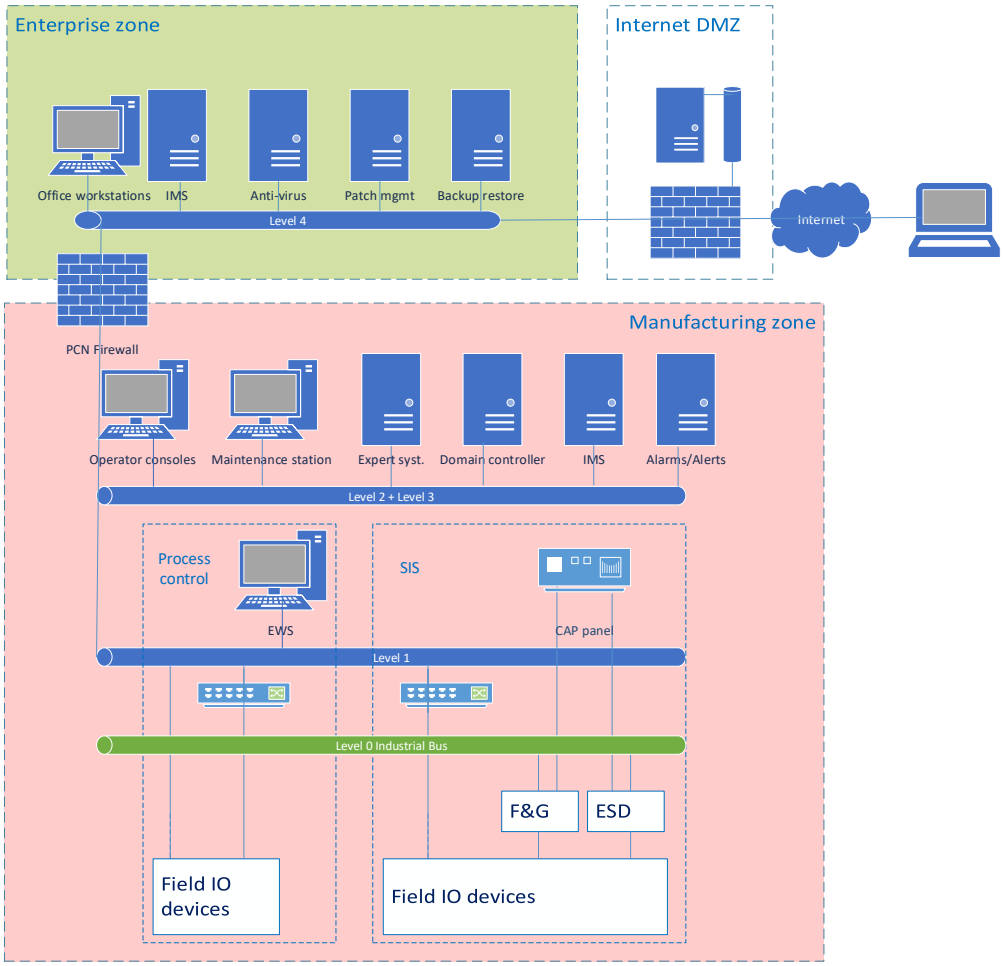
Man ønsket også å redusere kostnader knyttet til felt-kabling, vedlikehold og utvidelser, samt å muliggjøre distribuert prosessering og I/O. Det ble derfor introdusert industrielle nett (som beskrevet i Faktaboks 2) mellom sensorer, aktuatorer og styringssystemer.

I denne perioden ble det bygd ut fiberoptiske nett til et stort antall installasjoner på sokkelen og satellittbaserte kommunikasjonsløsninger for datatrafikk ble tilgjengelig. Noen installasjoner var også innenfor rekkevidden for radiolinje samband fra land eller naboinstallasjoner.

Mange av disse installasjonene har gradvis tatt i bruk sikkerhetsfunksjonalitet som beskrevet i kapittel 4.3.

4.2.1 Infrastruktur

Figur 2 viser skjematisk prinsippene for infrastruktur for nyere system. Figuren er basert på Purdue modellen som er beskrevet i Faktaboks 1.



Figur 2 – Infrastruktur og grensesnitt for nyere systemer

4.2.2 Nettverk og kommunikasjon

Det er etablert nettverksforbindelser mellom IKT-systemer og industrielle kontroll- og sikkerhetssystemer. Det overføres produksjonsdata fra industrisystemer til IKT-systemer og det tillates innlogging fra IKT-systemene til kontroll- og sikkerhetssystemene for vedlikehold. Eksterne leverandører gis temporær tilgang via internett.

Innen de industrielle kontroll- og sikkerhetssystemene er det lite separasjon av nett, typisk ett flatt nettverk på nivå 1, 2 og 3 for tilknytning av kontrollere, arbeidsstasjoner (EWS), kontrollrom samt i noen grad for tilknytning av tredjeparts systemer. Den vanligste måten for tilkobling av tredjeparts systemer er imidlertid ved hjelp av serielinjer (RS 232/485) med Modbus RTU som tilkobles kontrollere eller Modbus TCP.

Industrielle nett (som beskrevet i Faktaboks 2) for tilknytning av sensorer og aktuatorer er i liten grad benyttet for kritiske systemer i olje- og gass-sektoren. Dette forklares med at det var mye stabilitetsproblemer og vedlikeholdsproblematikk med driverprogramvare mm. som gjorde at man valgte direkte kablede forbindelser. For de industrielle nettene ble det først tatt i bruk Modbus RTU. Senere kom det en rekke nett på markedet som PROFIBUS, Modbus TCP, CANopen, PROFINET-IO, EtherNet/IO, EtherCAT og INTERBUS.

«Industrielle nett for tilknytning av sensorer og aktuatorer er i liten grad benyttet for kritiske systemer i olje- og gass-sektoren.»

For datainnsamling (se Faktaboks 4) er OPC-UA protokollen mye benyttet. Ettersom OSIsoft har en stor markedsandel, blir deres proprietære PI Connector mye benyttet.

Mellom installasjonene på Gullfaks feltet ble det lagt fiberoptisk kabel, og fiberoptiske kabler ble lagt sammen med kraftkabelen fra Kollsnes til Troll A plattformen. Troll A gikk i produksjon i 1995 og flere av plattformens operasjoner ble fjernstyrt fra land. Dette ble starten på utbygging av fibernett som i dag dekker store deler av installasjonene i Nordsjøen. Et fiberoptisk nett mellom Troll A og installasjonene i Tampen-område be skilt ut til selskapet Tampnett som senere har blitt en stor nettleverandør på sokkelen.

Industrielle datanett

Industrielle datanett er introdusert på 90-tallet for å spare kabel og installasjonskostnader samt å forenkle vedlikehold, dokumentasjon og utvidelser. De skulle også muliggjøre økt funksjonalitet ved å kunne distribuere prosesseringskraft. De første nettene («feltbusser») var basert på leverandørspesifikk teknologi, men skulle muliggjøre samspill mellom komponenter fra forskjellige leverandører.

Mange av dagens industrielle datanett er basert på Ethernet. Noen nett som f.eks. Modbus/TCP, EtherNet/IP og PROFINET RT benytter standard Ethernet, mens nett som PROFINET IRT og EtherCAT benytter et modifisert Ethernet for å forbedre sanntids ytelse. IEEE har etablert en TSN gruppe for å standardisere slike utvidelser.

Trådløse nettløsninger for industrielle nett er også tilgjengelig noe som ytterligere forenkler kabling. Nye prosjekter («Greenfield») er typisk kablet, mens ikke kritiske utvidelser og endringer ofte utføres med trådløse forbindelser. Trådløse industrielle nett benyttes også for temporære sensorer.

Bruk av felles industrielle nett som kan transportere TCP/IP kan utgjøre større risiko for IKT-sikkerhetshendelser.

Faktaboks 2 Industrielle datanett

4.2.3 IKT-sikkerhet

Det er satt opp en brannvegg mellom IKT-systemer og industrielle kontroll- og sikkerhetssystemer for å begrense datatrafikk.

Det er økende bruk av antivirus-kontroll på Windows-baserte industrielle kontroll- og sikkerhetssystemer.

SAS leverandørene foretar periodiske oppdateringer av sin programvare («patching»), ofte med portable lagringsmedier. Oppdatering av tredjeparts systemer er ofte manglende.

De store operatørselskapene utarbeidet selskapsinterne krav og veiledninger for IKT-sikkerhet.

Norsk Olje og Gass koordinerte utarbeidelsen av NOG 104 /3/ som var basert på ISO 27001 /4/.

Lysneutvalget /21/ kartla de digitale sårbarhetene i olje- og gassektoren i 2015. Dette kan representere sårbarheter i forhold til IKT-sikkerhet for de «nyere systemene»:

- Manglende oppmerksomhet og opplæring hos de ansatte
- Fjernarbeid (Det benyttes bl.a. usikre løsninger for fjernvedlikehold av PCer (f.eks. TeamViewer og pcAnywhere)
- Bruk av standardprodukter med kjente sårbarheter i produksjonsmiljø (f.eks. Windows XP)
- Mangelfull sikkerhetskultur hos underleverandører
- Mangel på separasjon av datanett.
- Manglende sikring av mobile lagringsenheter (inklusive smarttelefoner)
- Manglende sikring av datanett mellom landinstallasjoner og oljefelt
- Manglende fysisk sikring av datarom, kablingsskap, m.m.
- Sårbar programvare
- Utdaterte styresystemer på installasjoner (inklusive mangelfull «patching»)

Løsepengevirus

Løsepengevirus er en type ondsinnet programvare som truer med å publisere eller å blokkere tilgang til data med mindre det innbetales løsepenger. Løsepengene skal vanligvis innbetales i kryptovaluta (bitcoin) for at mottaker ikke skal kunne identifiseres. Data blokkeres vanligvis ved at de krypteres og ved innbetaling av løsepenger, skal det gis tilgang til krypteringsnøkkel.

Den ondsinnede programvaren NotPetya rammet en rekke industrielle installasjoner inklusive olje- og gassektoren i 2017. Windows baserte systemer stoppet og måtte reinstalleres. Boreinstallasjonene til Maersk var bl.a. utilgjengelig i 6 dager; noe som medførte vesentlige økonomiske tap og tap av omdømme. NotPetya viste seg å være en sletteorm («Wiperware») ettersom innbetaling av løsepengene ikke medførte at data kunne gjenskapes. LockerGoga er et løsepengevirus som angrep Hydro i 2019.

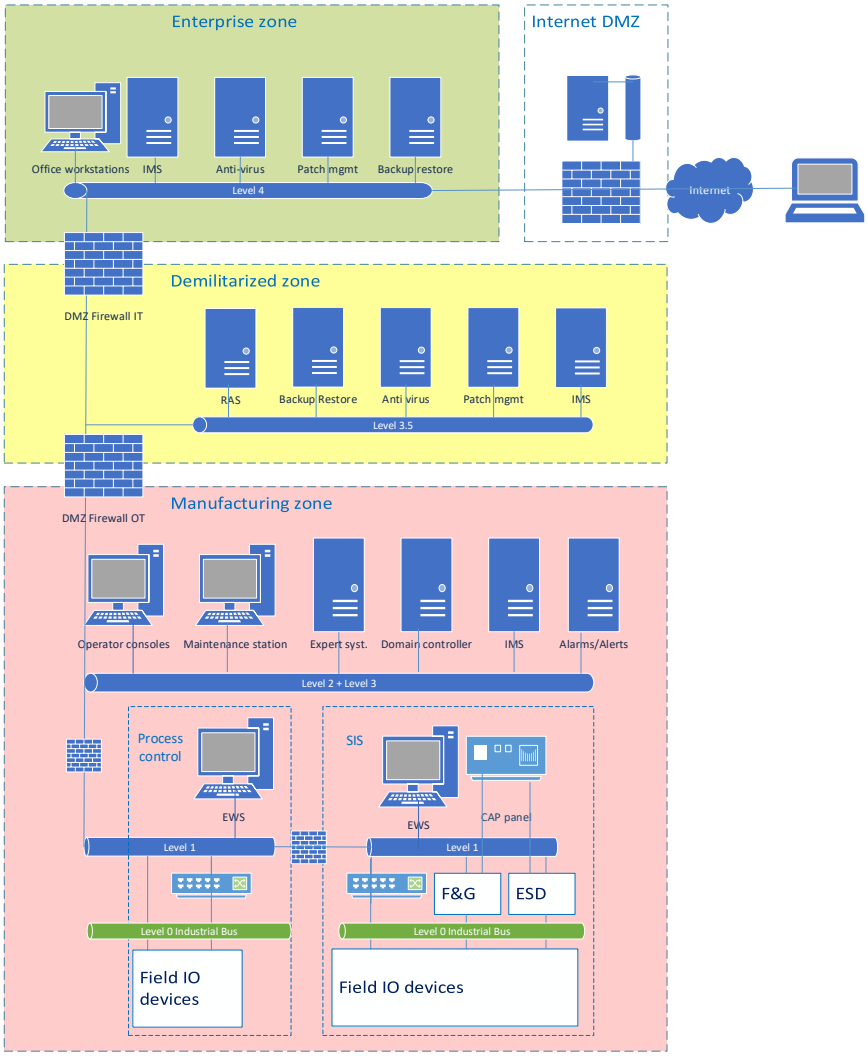
Faktaboks 3 Løsepengevirus

4.3 Dagens beste praksis

For å redusere sårbarhetene som beskrevet i kapittel 4.2.3, er infrastruktur for nybygg forbedret. Flere eksisterende installasjoner er også oppgradert. Er rekke aktører i sektoren samarbeidet med å dokumentere denne «beste praksis» basert på IEC 62443. Dette arbeidet ble dokumentert i DNVGL-RP-G108 /5/.

4.3.1 Infrastruktur

Infrastrukturen som vist i Figur 3 viser en demilitarisert sone mellom IKT-systemer og industrielle kontroll- og sikkerhetssystemer. Hovedhensikten med denne sonen er å ikke tillate direkte forbindelser. Anvendelser av denne demilitariserte sonen er beskrevet i Faktaboks 4 Datainnsamling og i Faktaboks 5 Fjerntilgang. I infrastrukturen er det også oppfordret til å gjøre en oppsplitting i soner og definere forbindelser basert på risikoanalyse. Sikkerhetskrav til de forskjellige soner og forbindelser settes basert på sikkerhetsnivåene i IEC 62443 standarden /7/. Sikkerhetssystemer skal separeres fra kontrollsystemer som beskrevet i Faktaboks 8 Separasjon av industrielle kontrollsystemer fra sikkerhetssystemer.



Figur 3 – Infrastruktur og grensesnitt, dagens beste praksis

4.3.2 Nettverk og kommunikasjon

Figur 3 viser en løsning med to brannvegger, en som skiller DMZ fra IKT, og en som skiller DMZ fra industrielle kontroll- og sikkerhetssystemer. Noen praktiserer at disse skal være av forskjellig fabrikat og at de skal opereres av forskjellige organisasjoner. Kritiske sektorer som f.eks. atomkraftindustrien har tatt i bruk data-dioder eller «uni-directional gateways» for å redusere risiko.

Figuren viser også en brannvegg mellom nivå 1 og nivå 2, men det er få installasjoner som har tatt i bruk en slik brannvegg. Det er vanlig at feltbusser er adskilt fra andre industrielle nettverk ved at kontrollerne (f.eks. PLS) fungerer som «dual hosts». De er tilkoblet både feltbusser på nivå 0 og et redundant Ethernet-basert nettverk til høyere nivåer.

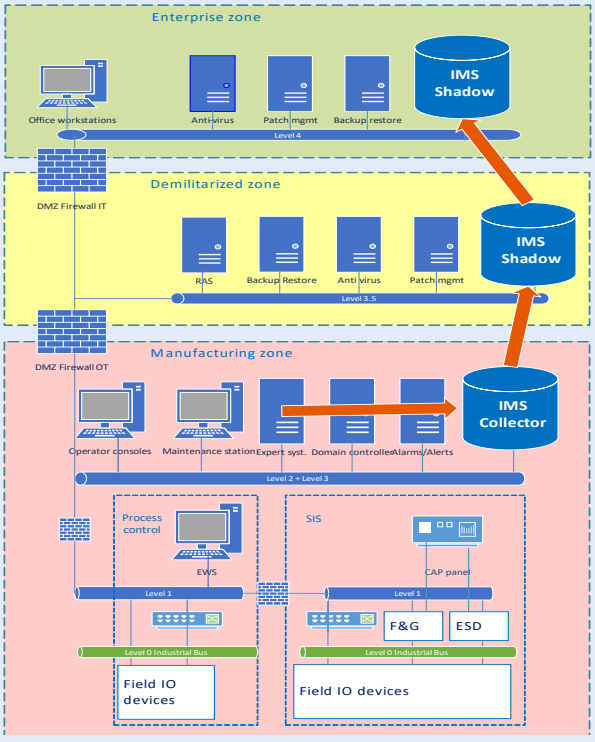
Det er økende bruk av sensorer med trådløs kommunikasjon. Et typisk trekk er at nye installasjoner («greenfield») har kablede nett, mens senere ikke kritiske endringer og spesielt temporære sensorer kommuniserer trådløst. Det er kjørt prosjekter med trådløse gass-detektorer som har vist god stabilitet. Det er varierende tiltro til batteribruk. Noen velger å kable for strømforsyning, mens andre baserer seg på batteriskifter. Batterier i trådløse sensorer skal typisk vare 1-2 år, men ustabiliteter i nett mm. vil kunne redusere denne tiden betraktelig.

Et typisk trekk er at nye installasjoner («greenfield») har kablede nett, mens senere ikke kritiske endringer og spesielt temporære sensorer kommuniserer trådløst.

For trådløs kommunikasjon benyttes primært WirelessHART (IEEE 802.15.4 / HART 7), ISA 100.11a og proprietære løsninger som Trusted Wireless (Phoenix Contact).

Blåtann (IEEE 802.15.1) og WiFi (802.11) er i liten grad benyttet på grunn av sensitivitet for støy.

Datainnsamling



Løsninger for innsamling, tilgjengeliggjøring og analyse av produksjonsdata er etablert for alle moderne olje- og gassinstallasjoner. Beste praksis for å sikre slike løsninger er å etablere en innsamlingsnode på nivå 3. Data repliseres en vei til en skyggeinstallasjon i demilitarisert sone, og repliseres deretter videre en vei til en skyggeinstallasjon på nivå 4.

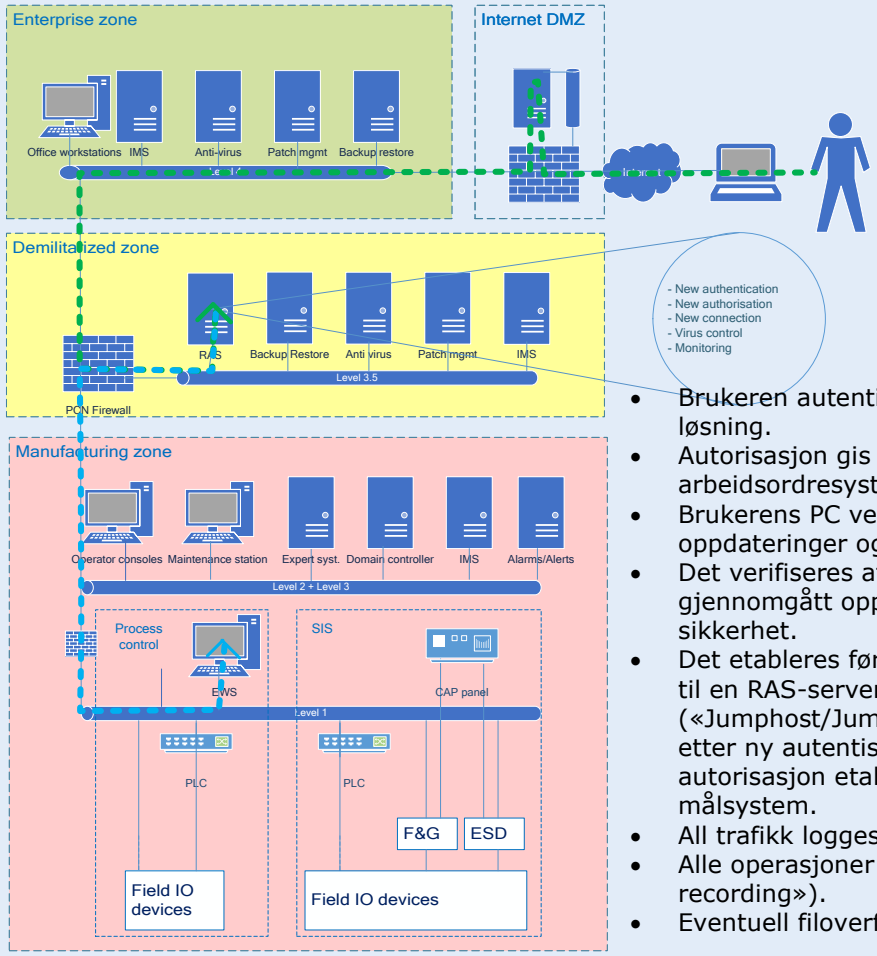
Brukere skal kun gis tilgang til data på nivå 4.

Brannvegger skal kontrollere datatrafikk i kun en retning. Data-dioder er et sikrere alternativ som muliggjør at IMS løsningen kan opprettholdes selv om brannvegg stenges i grunnet sikkerhetshendelser.

OPC-UA har etablert seg som en leverandøruavhengig protokoll for slik dataoverføring. Ettersom OSIsoft har en stor markedsandel, er det utstrakt bruk av deres proprietære PI Connector.

Faktaboks 4 Datainnsamling

Fjerntilgang

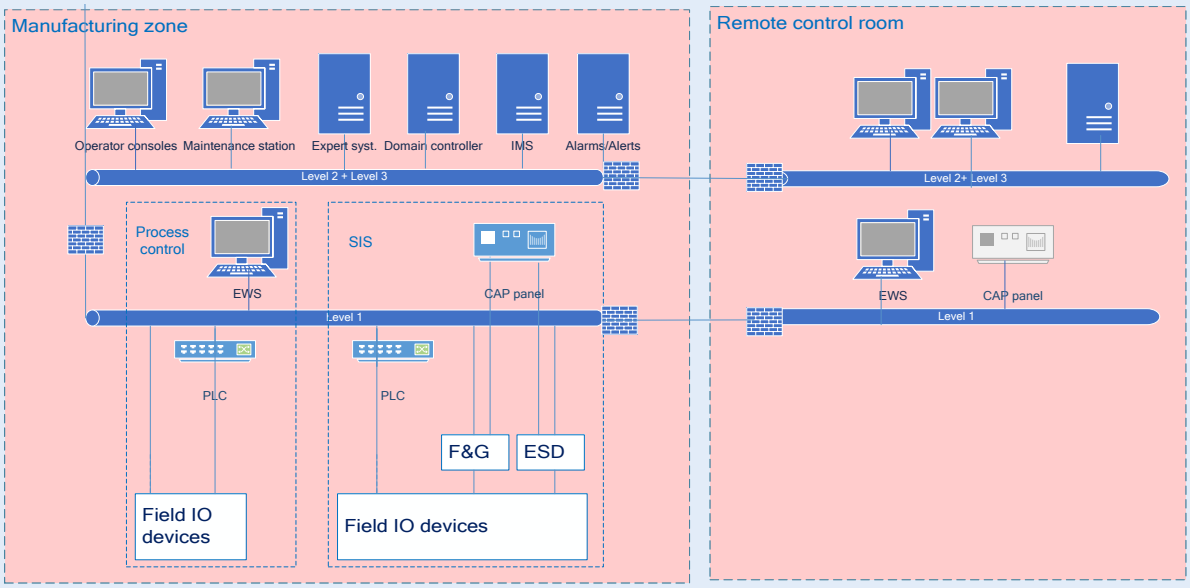


For å spare tid og kostnader ved reise ut til installasjoner, tillates fjerntilgang for vedlikehold. Slik tilgang via internett utgjør en stor risiko for IKT-sikkerhetshendelser og må sikres etter beste praksis:

- Brukeren autentiseres med to-faktor løsning.
- Autorisasjon gis basert på arbeidsordresystemet.
- Brukerens PC verifiseres i forhold til oppdateringer og antivirus.
- Det verifiseres at bruker har gjennomgått opplæring i IKT-sikkerhet.
- Det etableres først en kryptert tunell til en RAS-server («Jumphost/Jumpserver») i DMZ og etter ny autentisering og autorisasjon etableres ny tunell til målsystem.
- All trafikk logges.
- Alle operasjoner lagres («session recording»).
- Eventuell filoverføring virusvaskes.

Faktaboks 5 Fjerntilgang

Kontrollrom på land eller annen installasjon



Kontrollrom for mindre installasjoner som kompressorstasjoner legges til naboplattform eller til land. Det er planer om å ha ubemannede kontrollrom også på større installasjoner.
Nettverkene på lag 1, 2 og 3 (Se Faktaboks 1 om Purdue modellen) forlenges til fjerntliggende kontrollrom med krypterte tuneller. Slike tuneller kan sikre konfidensialitet og integritet, men ikke tilgjengelighet. Det må etableres tilstrekkelig redundante forbindelser. Det fjerntliggende kontrollrommet sikres fysisk og tilgang til rommet kontrolleres med f.eks. adgangskort.
Eventuelle dataforbindelser ut av fjerntliggende kontrollrom må sikres tilsvarende forbindelser ut av sone 1-3 på plattform.
Det er omdiskutert om det skal være CAP («critical action panel») på fjerntliggende kontrollrom. Dersom dette skal etableres, er det en god praksis å ha nøkkellåser som krever at både ansvarlig på plattform og ansvarlig på fjerntliggende kontrollrom åpner for bruk av et slikt CAP.

Faktaboks 6 Kontrollrom på land eller annen installasjon

4.3.3 IKT-sikkerhet

Infrastrukturen som vist i Figur 3 har til intensjon å redusere flere av sårbarhetene som beskrevet i kapittel 4.2.3. Dette forutsetter at ikke bare tekniske tiltak, men også prosess og menneskelige tiltak er implementert. Det forutsettes at det gjøres tilstrekkelig verifikasjon av sikkerhetstiltak knyttet til produksjonsstart og at tiltakene opprettholder ytelse over tid. Tiltakene skal tilpasses et endrende trusselbilde. I denne sammenheng har risiko- og barrierestyring som benyttet innen sikkerhet, vist seg som et godt hjelpemiddel /6/.

IEC 62443 /7/ standarden vurderes som tilstrekkelig moden og oppfattes av de fleste som godt egnet under konsept-, design- og prosjektfasen. Kravene til styringssystem (62443-2-1) er under omarbeidelse og krav til å knytte organisasjonens modenhet til tekniske krav (62443-2-2) er under utarbeidelse. Dette gjør at noen operatører benytter NIST rammeverket /8/ for operasjonsfasen.

Det pågår en omskriving av NOG 104 /3/ til å støtte opp under NIST rammeverket.

Konkraft rapporten anbefaler at bransjen går sammen om å etablerer et felles arbeidsordresystem for å sikre en enhetlig praksis /9/.

Konfidensialitet og integritet i de trådløse nettene sikres med kryptering. I dag tilbyr de fleste produkter AES 128. Integritet sikres med HASH algoritmer og de fleste produkter støtter SHA 2. Autentisering av

endepunkter sikres vanligvis med digitale sertifikater. Det er stor skepsis til bruk av kryptering for de kritiske systemene. Dette skyldes økt kompleksitet og vanskelig feilsøking. Når f.eks. et digitalt sertifikat utløper vil normalt datatrafikken stoppe.

«Det er stor skepsis til bruk av kryptering for de kritiske systemene.»

Ondsinnet programvare angriper sikkerhetssystemer

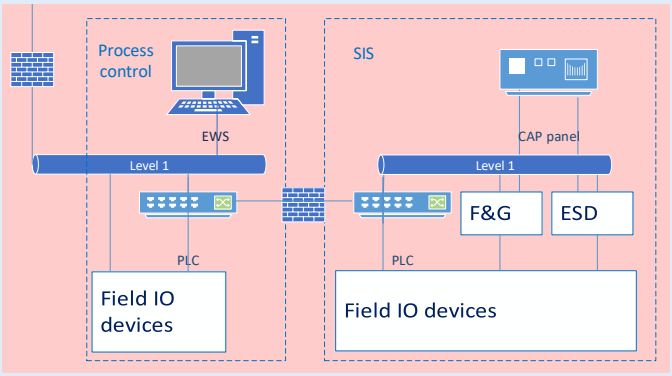
STUXNET fra ca 2010 var en øye-åpner for at industrielle kontrollsystemerer er sårbare for ondsinnet-kode. På samme måte var TRITON i 2017 en øyeåpner for at sikkerhetssystemer er sårbare. TRITON var antakelig den første ondsinnede koden som var laget for å skade et sikkerhetssystem. Det ble oppdaget etter et angrep mot et energiselskap i Midtøsten der en angriper fikk tilgang til en «engineering workstation» for et sikkerhetssystem og plantet skadevaren. Til alt hell, var det feil i koden slik at systemet stengte ned før angrepet gjorde omfattende skade.

TRITON (også kal TRISIS) er et rammeverk utviklet for å angripe Triconex Safety Instrumented System (SIS) kontrollere fra Schneider Electric. Det benytter Tristation protokollen for å sende kommandoer, lese minne og omprogrammere. Det kan eksempelvis stoppe enheten med en "halt" kommando.

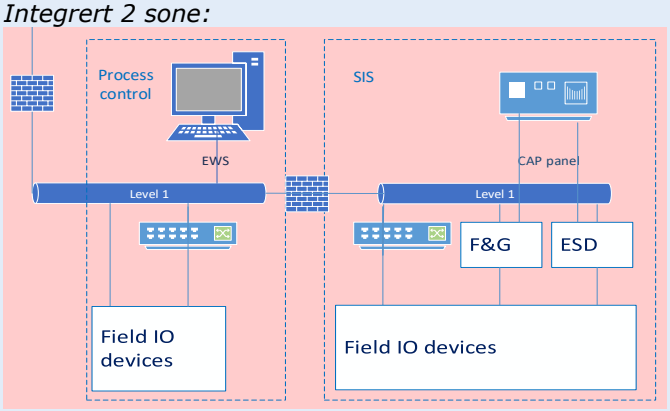
Faktaboks 7 Ondsinnet programvare angriper sikkerhetssystemer

Separasjon av industrielle kontrollsystemer fra sikkerhetssystemer

Tilkoblet:



Integrert 2 sone:



ISA TR-84 /22/ standarden beskriver fire prinsipper for å separere sikkerhetssystemer fra industrielle kontrollsystemer. Hensikten er å hindre at en IKT-sikkerhetshendelse som berører industrielle kontrollsystemer skal berøre sikkerhetssystemene:

Luft-gap – Både logisk og fysisk separasjon. Tillater dedikert kabling for tilstandsovervåkning.

Tilkoblet – Separat nett for PLS til PLS kommunikasjon. Tillater dedikert kabling for tilstandsovervåkning.

Integrert 2 sone – To avskilte nett med brannvegg. Kun les kommunikasjon fra sikkerhetssystem til kontrollsystem. Mulig å laste oppdateringer («pull») fra sikkerhetssystemer.

Integrert 1 sone - Begge systemer på samme nett. Muliggjør felles HMI, EWS mm. Krever andre tiltak for IKT-sikkerhet.

Faktaboks 8 Separasjon av industrielle kontrollsystemer fra sikkerhetssystemer

4.4 Forskjeller mellom innretninger, landanlegg og flyttbare rigger

I denne rapport er olje og gass innretninger, landanlegg og flyttbare rigger vurdert (Se kapittel 3.2).

Det er ikke identifisert store forskjeller i infrastruktur mellom faste og flyttbare rigger. Den vesentligste forskjellen er at tilkobling til eksternt fiberoptisk nett er enklere for faste innretninger enn for flyttbare. Flyttbare rigger med moderne rotasjonsledd («turrets») og sirkulære flytende innretninger (ikke roterende) har gjerne fibertilkoblinger.

Forskjellen i produkter og rutiner er stor mellom boreinstallasjoner og produksjonsinstallasjoner, men forskjellen i infrastrukturen for industrielle kontroll- og sikkerhetssystemer er liten.

Forskjellen i produkter og rutiner er stor mellom boreinstallasjoner og produksjonsinstallasjoner, men forskjellen i infrastrukturen for industrielle kontroll- og sikkerhetssystemer er liten.

For landanleggene, er det derimot identifisert vesentlige forskjeller:

Siden landanleggene har enklere transport av personell, opplever de en vesentlig høyere utskifting av personell spesielt hos underleverandører. Dette setter større krav til opplæring, kontroll, autentisering og autorisasjon.

Evakueringsmuligheter er vesentlig bedre for et landanlegg.

Landbaserte lagrings- og produksjonsanlegg kan ha store volumer av eksplosjonsfarlige stoffer som ikke raskt kan trykkavlastes i en nødsituasjon. Det anvendes derfor «seksjonalisering» i en nødsituasjon hvor trykkavlastning gjøres etter gitte sekvenser som er tilpasset dimensjoneringen av rørsystemer og faklingskapasitet. Dette medfører et mer komplekst nødavstengningssystem som må fungere over lengre tid, som eksekverer sekvensielle kontrollfunksjoner og som ikke utelukkende fungerer etter «fail-to-trip» prinsipper. Feil i sekvensielle nødavstengningssystemer kan medføre en storulykke. Løsningene krever også mer kommunikasjon på tvers av sikkerhetssystemer, strengere endringsrutiner og mer omfattende test og øvelse.

Feil i sekvensielle nødavstengningssystemer kan medføre en storulykke.

5 FREMTIDIGE TRENDER

Det er lansert en rekke trender og konsepter for å effektivisere olje- og gassektoren basert på bruk av IKT. «Digital Oilfield» er et generisk begrep for nye løsninger, teknologier, arbeidsprosesser og metoder basert på IKT. Andre navn som Integrerte Operasjoner (IO), «E-Field», «Smart Fields» og «i-field» brukes om det samme konseptet.

I dette kapittel diskuteres infrastruktur og IKT-sikkerhetsmessige konsekvenser av tingenes internett samt deler av digitaliseringstrenden knyttet til dataanalyse, simulering og prosessoptimalisering.

5.1 IIoT

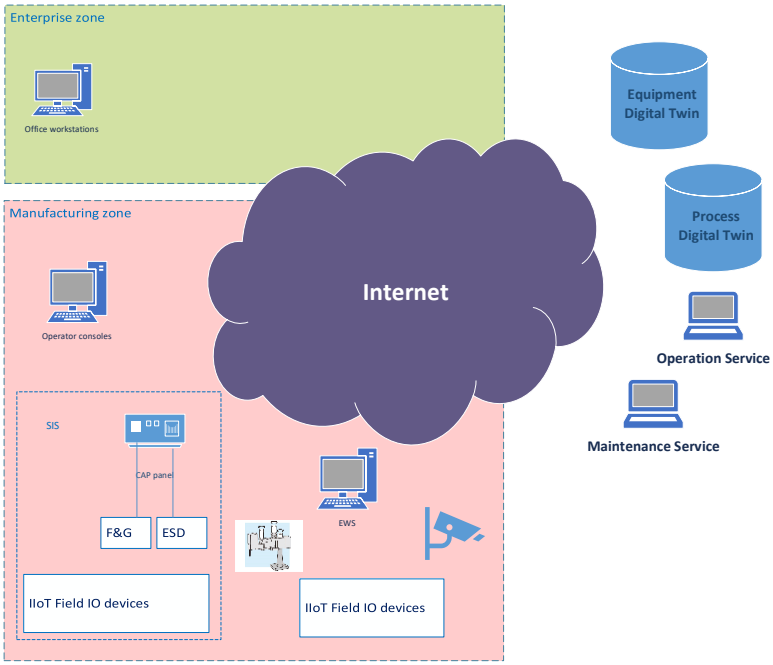
Termen «Industrial Internet of Things (IIoT)» kan fortolkes som den tekniske utviklingen at industrielle komponenter som f.eks. sensorer og aktuatorer i større og større grad utstyres med nettverkstilkobling (vanligvis Ethernet eller trådløs Ethernet) og at de får støtte for internettprotokollen TCP/IP. Eksempelvis har industrielle ventiler fått Ethernet grensesnitt, har innebygget web-server og kan styres fra en web-leser (Se Faktaboks 9).

En mer vanlig fortolkning av IIoT er at det inngår i en ny industriell revolusjon omtalt som «Industry 4.0» /10/ eller "Industrial Internet" som skal muliggjøre ett tett samspill mellom intelligente enheter («cyber physical systems»), avanserte analyse og mennesker. «Industry 4.0» er et begrep som referer til den fjerde industrielle revolusjon. Mens tredje industrielle revolusjon refererer til introduksjon av automatiseringssystem, refererer den fjerde industrielle revolusjon til utviskingen av skille mellom den fysiske, digital og biologiske verden /11/. Et slikt konsept vil bl.a. kombinere smarte sensorer og aktuatorer med analyse- og optimaliseringsressurser slik at produksjonsanlegg kan reagere i sann tid til endringer og hendelser som kan påvirke prosessen. Dette vil kunne optimalisere både volum og energiforbruk i olje- og gassindustrien. Videre vil et slikt konsept kunne forbedre proaktivt vedlikehold med kontinuerlig overvåkning av tilstand og redusere ikke planlagt nedetid. HMS vil forbedres eksempelvis ved at maskiner vil «se» menneskene og unngå sammenstøt på boredekk og under løfteoperasjoner.

Slik overvåkning og sentral datainnsamling gir mulighet for nye samarbeidsformer mellom operatør og leverandør slik man har sett i andre bransjer. I eksempelvis forsvarssektoren inngås det PBL (Performance Based Logistic) /12/ avtaler hvor leverandøren har ansvaret for tilgjengelighet. Slike forretningsmodeller kan også bli aktuelle i fremtidens olje- og gassvirksomhet.

Det finnes IIoT visjonærer som mener at infrastrukturen vil få dramatiske forenklinger. Siden de industrielle intelligente enhetene har full støtte for internettprotokoller og de mest avanserte og rimeligste analyseplattformene ligger i skyen, kan man se for seg en flat infrastruktur som vist i Figur 4. De sikkerhetsmessige utfordringene ved en slik flat infrastruktur er signifikante. (Se kapittel 5.1.3.) Frem til det er etablert sikkerhetsløsninger for IIoT enheter med akseptabel risiko, er det i sektoren en oppfatning av at eksisterende sonemodeller må opprettholdes som vist i Figur 5.

«Frem til det er etablert sikkerhetsløsninger for IIoT enheter med akseptabel risiko, er det i sektoren en oppfatning av at eksisterende sonemodeller må opprettholdes.»



Figur 4 – Teoretisk flat infrastruktur for IIoT

Eksempler på IIoT enheter for olje- og gass-sektoren

Sensorer for roterende utstyr: Roterende utstyr som kompressorer, strømgeneratorer, pumper, vifter mm krever store ressurser til vedlikehold. Kontinuerlig overvåkning og analyse er et effektivt hjelpemiddel for å detektere avvik, samt å styre vedlikeholdsintervaller. Vibrasjons-sensorer, hastighetssensorer og akselerasjonssensorer er viktige givere til denne overvåkningen og analysen. Slike sensorer utstyres nå med nettverksgrensesnitt (f.eks., Trådløs Ethernet) og kommuniserer med internettprotokoll (f.eks. MQTT).

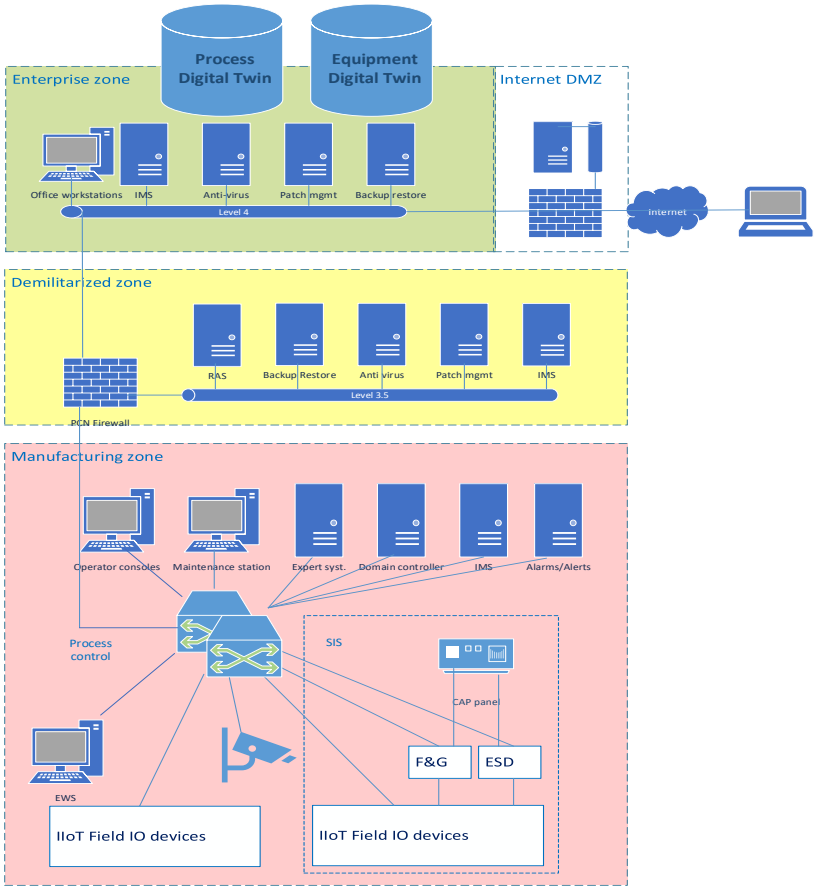
Trådløse gassdetektorer: Det er gjennomført flere prosjekter i Nordsjøen for å teste trådløse gassdetektorer. Detektorene er konfigurert som et trådløst maskenettverk og kommunikasjonen skjer ved bruk av ISA100.11a-protokollen med et Profisafe lag på toppen. Profisafe-laget sikrer punkt-til-punkt-sertifisert kommunikasjon i henhold til pålitelighetskravene (SIL2) og gir full integrasjon til kontrollsystem (PLS). Prosjektene har vist at installasjon av slike enheter ble gjort på vesentlig kortere tid enn trådbundne systemer samtidig som stabilitet har vært like god.

Ventiler med IIoT: Tradisjonelle ventiler kan i dag leveres med innebygget nettverksstøtte og støtte for internettprotokoll. Flere ventiler har også innebygget web-tjener og kan styres fra en web-leser. (Dette kan utgjøre en sikkerhetsrisiko, og må sikres eller slås av.)

Faktaboks 9 Eksempler på IIoT enheter for olje- og gass-sektoren

5.1.1 Infrastruktur

Figur 5 viser en mulig fremtidig infrastruktur for IIoT i olje- og gass-sektoren. Figuren viser at kontrollere, sensorer og aktuatorer som støtter internettprotokollen kommuniserer direkte mot en dublert svitsjet nettverksstruktur på lag 1-3. Videre vises nye sensorer og overvåkningsutstyr koblet mot den samme infrastrukturen. Kritiske sikkerhetssystemer vil ha egne kontrollere fremdeles fast kablet mot sensorer og aktuatorer.



Figur 5 – Infrastruktur og grensesnitt for IIoT

5.1.2 Nettverk og kommunikasjon

IIoT enheter vil definisjonsmessig kommunisere basert på internettprotokoll dvs. TCP/IP. Enhetene er utstyrt med enten Ethernet grensesnitt eller industrielle nett, og det forventes økende bruk av trådløse forbindelser. For ikke industrielle miljø (IoT) forventes mye bruk av kommunikasjonsløsninger for batteristrømdrevne enheter (f.eks. Zigbee, Bluetooth LE eller LoRaWan), men disse er lite egnet i industrielle miljø. Hvilken protokoll som benyttes over TCP (eller UDP) er uklart. Det er flere kandidater som konkurrerer som beskrevet i Faktaboks 10 Protokoller for IIoT.

Det vil fremdeles være installasjoner som er avhengig av korte forutsigbare forsinkelser i nettet samt raske omkoblingstider ved feil/brudd. For slike installasjoner kan ikke standard Ethernet benyttes og

industrielle nett må brukes. For å kommunisere med andre IIoT enheter vil det da trengs overganger («gateways»). Flere slike «gateway» produkter er introdusert i markedet.

Det forventes utvidet bruk av virtuelle nett (VLAN) for å gi sikkerhetsmessig separasjon av virtuelle soner. Tilsvarende vil det bli utvidet bruk av prioriteringsmekanismer i nettet. Det er bekymring for at store datavolum fra eksempelvis overvåkningskamera og sensorer som lytter på roterende utstyr, skal forstyrre tidskritiske prosess-signaler.

«Det er bekymring for at store datavolum fra eksempelvis overvåkningskamera og sensorer som lytter på roterende utstyr, skal forstyrre tidskritiske prosess-signaler.»

Neste generasjon av nettverk for mobiltelefoner (5G) vil få funksjonalitet for å støtte IIoT. Dette inkluderer bedre sanntidsegenskaper. For ikke produksjonskritiske sensorer vil dette kunne bli et alternativ også i olje- og gassindustrien. Tilsvarende gjøres det forbedringer av tradisjonelle nettverksprotokoller for IIoT enheter. MPLS-TP er en slik kommende forbedring som skal forbedre egenskaper for industrielle applikasjoner.

Protokoller for IIoT

Det er ikke etablert en standardprotokoll for kommunikasjon med IIoT enheter. Det er lansert flere alternativer/kombinasjoner. Noen av disse er:

OPC-UA
Open Platform Communications Unified Architecture ble lansert i 2006 og har etablert seg som en de-facto standard for leverandøruavhengig datainnsamling (Se Faktaboks 4 Datainnsamling). Arkitekturen er en videreutvikling/tilpasning av Microsoft COM/DCOM for industriell automasjon. OPC-UA oppfattes som funksjonsrik og har god utbredelse, men arven fra COM/DCOM gjør den kompleks og ressurskrevende for utviklere. OPC-UA kan benytte MQTT og AMQP for datatransport.

MQTT
MQ Telemetry Transport ble utviklet av IBM i 1999. MQTT er en klient-tjener «publish/subscribe» meldingsprotokoll. Protokollen krever lite ressurser i nodene og skal være enkel å implementere. MQTT har nylig blitt en OASIS standard. (MQ Series var navnet på et IBM produkt og dette har gitt en feilaktig oppfatning om at MQTT er en Message Queue protokoll)

AMQP
Advanced Message Queuing Protocol ble utviklet i 2003 av John O'Hara. AMQP er en åpen standard for meldingsbasert mellomvare.

Faktaboks 10 Protokoller for IIoT

5.1.3 IKT-sikkerhet

I olje- og gass sektoren er en bekymret for IKT-sikkerhet ved innføring av IIoT enheter. Disse bekymringene stammer primært fra ikke industrielle enheter (IoT) der det er avdekket en rekke sårbarheter. Dersom man skal forenkle sonemodeller og tillate direkte kommunikasjon mellom IIoT-enheter (se Figur 4), må det etableres sikker oppstart av noder («boot code»), sikker oppdatering («patching»), node autentisering og sikre kommunikasjonsprotokoller. I praksis må det etableres ende-til-ende kryptering og autentisering med f.eks. digitale sertifikat. Det er stor skepsis til å innføre kryptering og sertifikater innen industrielle kontroll- og sikkerhetssystemer grunnet både ytelse og tilgjengelighet. Ytelsesproblematikken forventes å bli løst med nye og raskere enheter, men gamle systemer vil ikke ha tilstrekkelig kapasitet. Tilgjengelighetsproblematikken gjenstår å løses ettersom innføring av kryptering og sertifikater øker kompleksiteten vesentlig. Når f.eks. et digitalt sertifikat

utløper vil kommunikasjonen normalt stoppe. Det er videre vanskelig å feilsøke med krypterte protokoller.

«Det er stor skepsis til å innføre kryptering og sertifikater innen industrielle automasjon og sikkerhetssystemer grunnet både ytelse og tilgjengelighet.»

IIoT enheter er ofte basert på sanntidsoperativsystem (f.eks. TreadX, Nucleus eller Linux varianter). Disse operativsystemene kan mangle sikkerhetsfunksjonalitet.

5G nettene inkluderer kryptering fra node til base-stasjon, men har ikke ende-til-ende kryptering. Dette må implementeres i applikasjonsprotokoller.

5.2 Dataanalyse, simulering og prosessoptimalisering

Mengden av data som transporteres fra industrielle systemer til IKT-systemer (Se Faktaboks 4) har vært sterkt økende over lang tid. Det hevdes at volumet fordobler seg hvert 1,2 år. Samtidig estimeres at kun 1-2% av data fra ca. 30.000 sensorer på en oljeinstallasjon benyttes for beslutningsstøtte /13/. Moores lov /14/, som sier at prosessor og prosesseringskapasitet fordobles hver 18 måned, har bevist sin gyldighet gjennom 50 år. Det er dermed forventet en vesentlig øking i datavolumer og prosesseringskapasitet fremover.

Dagens olje- og gassinstallasjoner er helt avhengige av manuell overvåkning og kontroll fra høyt kvalifisert personell i kontrollrom. For å utdanne nye kontrollromsoperatører og for å trene slikt personell på uforutsatte hendelser, er det lagt ned store ressurser i etablering av simulatorer. De aller fleste installasjonene har etablert simulatorer som ideelt skal være fullverdige «kopier» av produksjonsanlegget. Slike simulatorer har også vært et nyttig hjelpemiddel for å teste ut endringer som f.eks. programvareoppdateringer og sikkerhetsrettelser («patcher») før de settes i produksjon.

Både behovet for bedre dataanalyse og behovet for simuleringsløsninger er drivere for digital tvilling konseptet. Mange aktører har begynt å rendyrke disse løsningene som digitale tvillinger. Denne prosessen krever en avklaring om prosesseringsressursene skal knyttet til produksjonsanlegget («edge computing») eller om ressursene skal leies hos en skyleverandør («cloud computing») (Se Faktaboks 11).

Digitale tvillinger har vært i bruk i olje- og gassektoren over mange tiår uten at begrepet har vært entydig definert. En digital reservoar-modell er en digital tvilling. Innen bore-virksomheten utarbeides nye konsepter for robot-boring der boreplaner utarbeides basert på simulering med digitale tvillinger av reservoar.

«Digitale tvillinger har vært i bruk i olje- og gassektoren over mange tiår uten at begrepet har vært entydig definert. En reservoar-simulering er en digital tvilling.»

Dataanalyse og simuleringer vil kunne beregne optimale prosessinnstillinger. I dag brukes primært manuelle rutiner for at kontrollromsoperatører kan implementere disse innstillingene. For å få full effekt av analyse og simuleringsløsningene er det et sterkt ønske om å kunne utføre disse prosessoptimaliseringene automatisk og i sann tid. Dette gir store sikkerhetsutfordringer. Så lenge data transporteres en vei fra industrisystemer til IKT-systemer for analyse og simulering, oppfattes at dagens beste praksis for informasjonssikkerhet (Se kapittel 4.3) gir akseptabel risiko. Tilstrekkelig sikre løsninger for å transportere kritiske prosessdatadata den motsatte vei er ikke implementert.

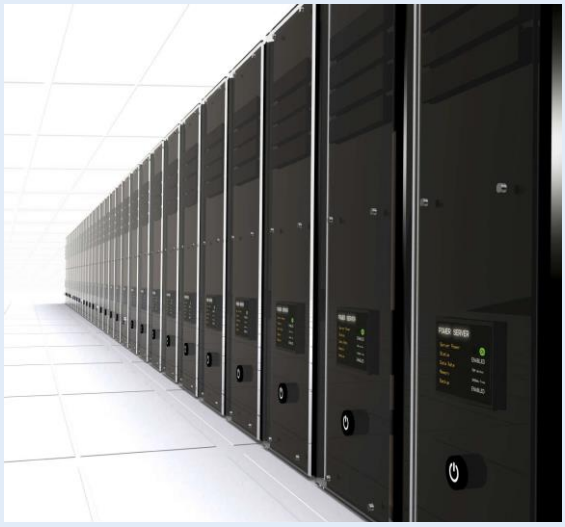
«For å få full effekt av analyse og simuleringsløsningene er det et sterkt ønske om å kunne utføre disse prosessoptimaliseringer automatisk og i sann tid. Dette gir store sikkerhetsutfordringer.»

Fokus på prosessoptimalisering vil fortsette og bli mer knyttet til eksterne faktorer som for eksempel strømpriser, klima, samfunnsøkonomi og internasjonale avtaler. Det antas at slike eksterne komplekse kontrollstrategier vil direkte påvirke olje- og gass produksjon, lagring og eksport på lik linje som mer tradisjonelle optimaliseringsmål som HMS, vedlikehold og produksjonskostnader.

Nye forretningsmodeller er introdusert i sektoren hvor leverandører selv får ansvar for å samle inn, overvåke, vedlikeholde og forbedre eget utstyr. Dette vil nødvendiggjøre at leverandørene får direkte tilgang til sensordata og innsamlet historikk samt mulighet til å oppdatere egen programvare. Flere aktører med tilgang til kritiske produksjonssystemer vil øke eksponeringen for inntrengning og skadelig programvare.

Det er et stort trykk på bransjen om kostreduksjon, spesielt ved økt digitalisering og bedre samarbeid. Dette kommer blant annet til uttrykk i Konkraft anbefalingene fra 2018. I Konkraft rapporten foreslås en rekke forbedrings og besparelsestiltak for sektoren. Mange av disse forutsetter at informasjon gjøres tilgjengelig for aktørene som i skyløsninger /9/.

Lokale tjenester versus skytjenester



Det er en pågående diskusjon om prosesseringsressurser skal etableres lokalt knyttet til produksjonsanlegget («Edge Computing») eller om prosesseringsressurser skal leies som en skytjeneste («Cloud computing»). I prinsipp er dette en diskusjon om kontroll og tilgjengelighet mot pris, kapasitet og mulighet for å dele data. «Edge Computing» muliggjør bedre kontroll med både konfidensialitet, integritet og tilgjengelighet. Løsningen vil i mindre grad være avhengig av eksterne datanett. Kostnad knyttet til prosesseringskraft inklusive drift og vedlikehold vil normalt være vesentlig lavere ved «Cloud computing». Skytjenester enten som privat sky eller som offentlig sky prefereres ved etablering av felles-modeller for flere installasjoner.

Faktaboks 11 Lokale tjenester versus skytjenester

5.2.1 Infrastruktur

Se kapittel 5.1.1.

5.2.2 Nettverk og kommunikasjon

Se kapittel 5.1.2.

5.2.3 IKT-Sikkerhet

Utover de sikkerhetsløsninger som er dokumentert i kapittel 5.1.3, er det forventninger til at to nye kryptobaserte teknologier skal kunne sikre analyse, simulering og prosessoptimalisering i skytjenester:

Blokk-kjeder («Blockchain»)

Blokk-kjeder /18/ kan sikre integritet, ikke-benekt og konfidensialitet for data som prosesseres i en kjede av prosesser/aktører. En slik teknologi kan sikre at prosessinnstillinger og produksjonsdata sendes

til en ekstern aktør for analyse og prosessoptimalisering. Optimaliserte prosessinnstillinger kan deretter sendes tilbake til produksjonsanlegget med visshet om at de nye verdiene bygger på opprinnelige data og at kun tiltrodd analyseaktør har modifisert data. Data kan sikres mot innsyn under overføring.

«Homomorphic encryption»

«Homomorphic encryption» /19/ er et konsept som muliggjør matematiske operasjoner på krypterte data. Det betyr at en skyleverandør kan motta krypterte data, gjøre analyse og optimalisering på de krypterte data og overføre resultatene tilbake til prosess. Teknologien er pr. i dag umoden, men det forventes at teknologien vil gi stor betydning for å sikre konfidensialitet i skytjenester.

6 REFERANSER

/1/ SINTEF, 2018: Kunnskapsprosjekt IKT-sikkerhet; Industrielle kontroll- og sikkerhetssystemer i petroleumsvirksomheten: https://www.ptil.no/fagstoff/utforsk-fagstoff/prosjektrapporter/prosjektrapporter-2019/industrielle-kontroll--og-sikkerhetssystemer-i-petroleumsvirksomheten/

/2/ Theodore J. Williams, 1992: The Purdue enterprise reference architecture: a technical guide for CIM planning and implementation. Research Triangle Park, NC: Instrument Society of America.

/3/ Norsk olje & gass, 2013: 104 Anbefalte retningslinjer krav til informasjonssikkerhetsnivå i IKT-baserte prosesskontroll-, sikkerhets- og støttesystemer: https://www.norskoljeoggass.no/arbeidsliv/retningslinjer/integrerte-operasjoner/104-anbefalte-retningslinjer-krav-til-informasjonssikkerhetsniva-i-ikt-baserte-prosesskontroll--sikkerhets--og-stottesystemer-ny-revisjon-pr-05.12.2016/

/4/ ISO/IEC 27001, 2013: Information technology - Security techniques - Information security management systems - Requirements. International Organization for Standardization.

/5/ DNVGL-RP-G108, 2017: Cyber security in the oil and gas industry based on IEC 62443 2013: https://www.dnvgl.com/oilgas/download/dnvgl-rp-g108-cyber-security-in-the-oil-and-gas-industry-based-on-IEC-62443.html

/6/ Prinsipper for barrierestyring i petroleumsvirksomheten, Petroleumstilsynet: http://www.ptil.no/getfile.php/PDF/Prinsipper%20for%20barrierestyring%20i%20petroleumsvirksomheten.pdf

/7/ IEC 62443-3-3, 2013. *Security for Industrial Automation and Control Systems, System Security Requirements and Security Levels.* International Electrotechnical Commission.

/8/ NIST, 2014: Framework for Improving Critical Infrastructure Cybersecurity: https://www.nist.gov/cyberframework

/9/ Konkraft, 2018: Konkraft rapport «Competitiveness – changing tide on the Norwegian continental shelf»- Summary and recommendations from the Committee.

/10/ BMBF-Internetredaktion, 2016: "Zukunftsprojekt Industrie 4.0 - BMBF"

/11/ World Economic Forum, 2015: Foreign Affairs

/12/ United States Department of Defense, 2018: Performance-based logistics

/13/ Mc Kinsey Global Institute, 2015: By 2025, Internet of things applications could have $11 trillion impact

/14/ Electrics magazine, 1965: Cramming more components onto integrated circuits

/15/ IEEE Industrial Electronics Magazine, 2017: The Future of Industrial Communication

/16/ Renesas, 2016: Device Security for the IIoT

/17/ Schneider Electric, 2016: Industrial Internet of Things (IIoT) Impact on the Oil & Gas Industry Value Chain.

/18/ Narayanan, Arvind; Bonneau, Joseph; Felten, Edward; Miller, Andrew; Goldfeder, Steven, 2016: Bitcoin and cryptocurrency technologies: a comprehensive introduction.

/19/ Armknecht, Frederik; Boyd, Colin; Gjøsteen, Kristian; Jäschke, Angela; Reuter, Christian; Strand, Martin, 2015: A Guide to Fully Homomorphic Encryption.

/20/ Forskningsrapport 3/2015 Handelshøgskolen BI, 2015: Informasjon over Nordsjøen: Telekommunikasjoner på norsk sokkel.

/21/ Justis- og beredskapsdepartemen, 2015: NOU 2015:13 Digital sårbarhet – sikkert samfunn. Beskytte enkeltmennesker og samfunn i en digital verden

/22/ ISA-TR84.00.09, 2013. Security Countermeasures Related to Safety Instrumented Systems (SIS)

APPENDIX A INTERVJU KANDIDATER

Det er foretatt intervju med følgende aktører i olje- og gass-sektoren:

- ABB
- Aker BP
- Equinor
- Honeywell
- Lundin Norway
- MHWirth
- Norske Shell
- NOV Rig Technologies
- Odfjell Drilling
- Siemens
- Vår Energi

APPENDIX B INTERVJUGUIDE

Fase 1. Rammesetting (5 min)

- Ønske velkommen, presentasjon

2. Informasjon (10 min)

- Si litt om temaet for samtalen (bakgrunn, formål)
- Forklar hva intervjuet skal brukes til, nevn taushetsplikt og anonymitet
- Forklar rollene til personene fra DNV GL
- Spør om noe er uklart og om respondenten har noen spørsmål

Fase 3. Ansvar/Rolle: (10 min)

- Fortell litt om ditt arbeid og din rolle i organisasjonen
- Hva slags erfaringer har du med Industriell IKT og IIoT?
- Kan person eller organisasjon refereres i rapport?

Fase 4. Eksisterende infrastruktur: (30 min)

- Presenter skisser av «generasjonene»:
  - Stemmer dette med din oppfatning?
  - Hvordan vurderer du fordelingen av systemer i din organisasjon (dine prosjekter)?
- Er «eldre systemer» tilknyttet eksterne nett?
- Hvilke sikkerhetstiltak ble innført når de fikk nettilknytning?
- Hvilken sonemodell er implementert?
- Hva slags barrierefunksjoner mellom soner er etablert?
- Hva er status på herding og viruskontroll?
- Benyttes fjerntliggende kontrollrom?
- Benyttes fjernvedlikehold?
- Er det separasjon av nett mellom prosesskontroll og sikkerhetssystemer?

Fase 5. Industrielle nett (30 min)

- Ca. når ble industrielle nett innført?
- Hvilken type nett er etablert?
- Hvilken type enheter er tilknyttet de industrielle nettene?
- Benyttes trådløse nett for industrielle nett?

Fase 6. IIoT (30 min)

- Hva er status/planer om bruk av enheter med IIoT egenskaper?
- Hvordan vil disse knyttes opp i forhold til sonemodell?
- Hva er planer om andre sikringstiltak (kryptering, identifisering…)?

Fase 7. Analyse og optimalisering (30 min)

- Er det etablert felles system for IMS?
- Hva er status/planer i forhold til Digital Tvilling?
- Gjøres det analyse hos eksterne «skyleverandører»?
- Hva er strategi i forhold til «Cloud vs Edge computing»?

- Er det planer om å la analyseløsninger optimalisere IKT-løsninger?

Fase 8. Oppsummering (ca. 10 min)

- Oppsummere funn
- Har jeg forstått deg riktig?
- Er det noe du vil legge til? Nye intervjuobjekter, nye dokumenter?

About DNV GL

Driven by our purpose of safeguarding life, property and the environment, DNV GL enables organizations to advance the safety and sustainability of their business. We provide classification and technical assurance along with software and independent expert advisory services to the maritime, oil and gas, and energy industries. We also provide certification services to customers across a wide range of industries. Operating in more than 100 countries, our 16,000 professionals are dedicated to helping our customers make the world safer, smarter and greener.